

CIBERSEGURIDAD

'Bootcamp IX'

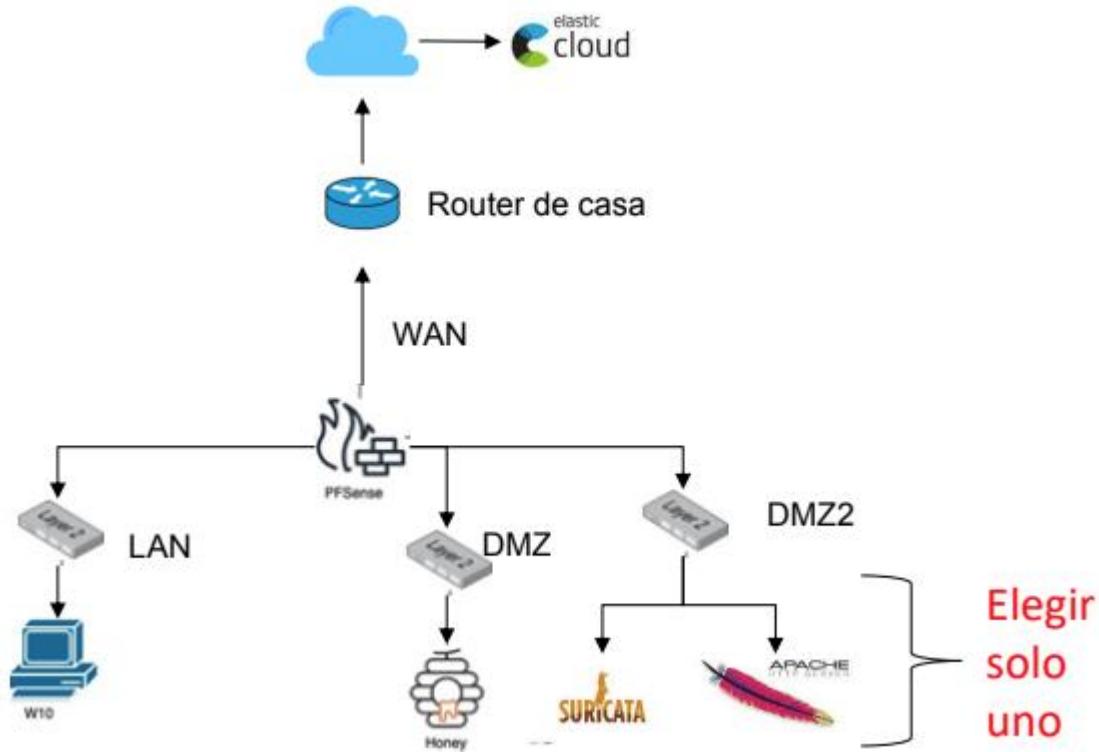
Informe Práctica Blue Team.

Maximiliano Dariel Altamirano.

Academia KeepCoding.

Enunciado:

Queremos montar la siguiente infraestructura:



Los requisitos que debe cumplir son los siguientes:

1. Debe tener un pfSense en que se interconecten las redes LAN, DMZ y DMZ2
2. En la red LAN debe haber un equipo Windows 11 que envíe logs al servidor de Elastic.
3. En la red DMZ debe haber un honeypot que envíe los logs al servidor de Elastic.
 1. Este honeypot no debe tener acceso a ninguna red interna (LAN, DMZ2...) y debe ser accesible desde el exterior (red WAN) en ambos sentidos.
4. En la red DMZ2 debe haber otra fuente diferente de logs a las dos mencionadas anteriormente. Se propone Suricata o Apache Server como posibles fuentes, pero se deja a elección del alumno.
5. El servidor de Elastic debe recibir, almacenar y poder visualizar los logs del honeypot, el Windows 11 y la fuente elegida ubicada en la DMZ2.

Criterios de evaluación de la memoria:

1. Debe contener evidencias y explicaciones que demuestren la correcta creación de la infraestructura de red en el pfSense.
2. Debe contener explicación y captura de las reglas de firewall elegidas para cada red (WAN, NAT, LAN, DMZ y DMZ2)
3. Debe contener evidencias de las políticas e integraciones asignadas a cada agente del SIEM (Elastic)
4. Debe contener evidencias que demuestren la correcta recepción de los logs, de todas las fuentes especificadas en el enunciado, en el SIEM (Elastic).



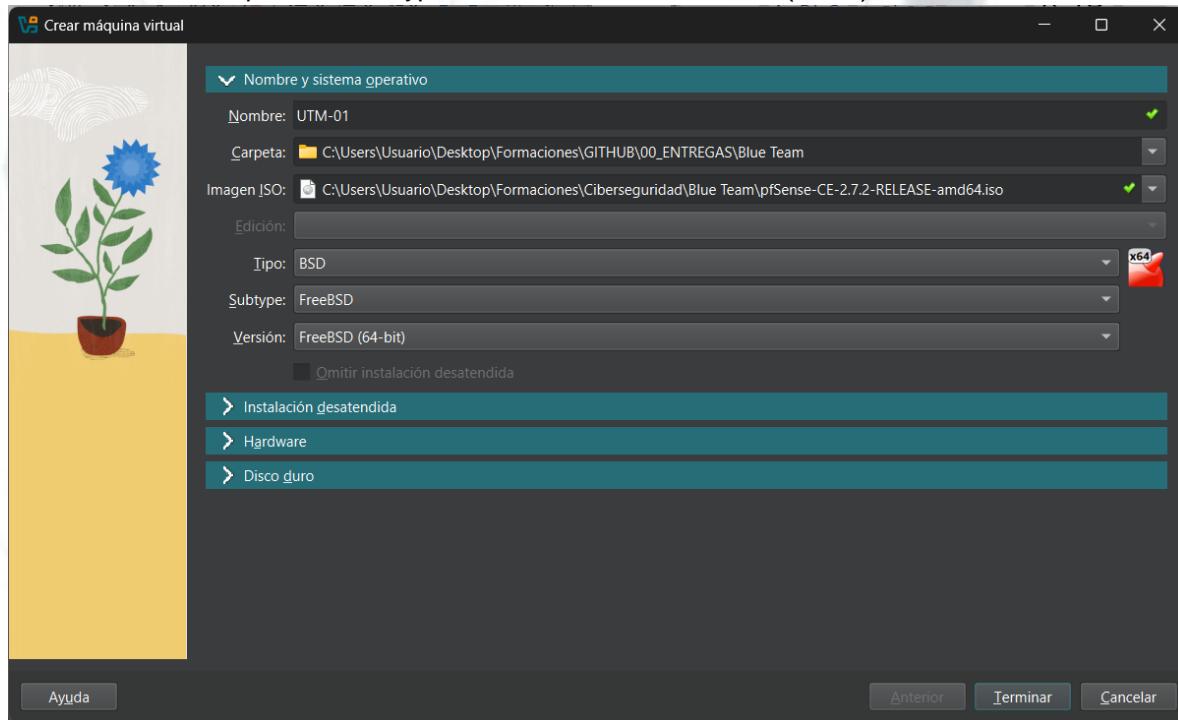
Desarrollo:

1. Debe tener un pfSense en que se interconecten las redes LAN, DMZ y DMZ2.

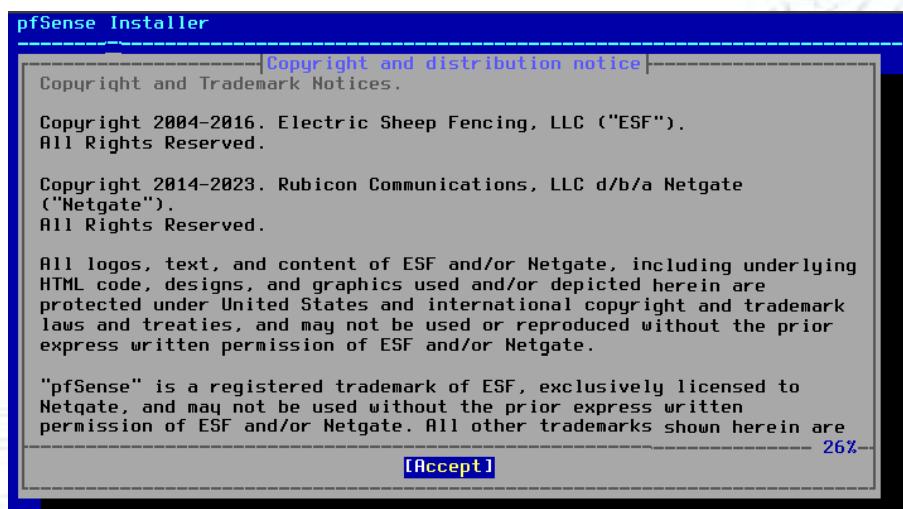
Comenzamos instalando y configurando el pfSense. Previamente deberemos disponer de un virtualizador (VirtualBox) y de la imagen ISO para generar nuestro UTM-01 (pfSense).

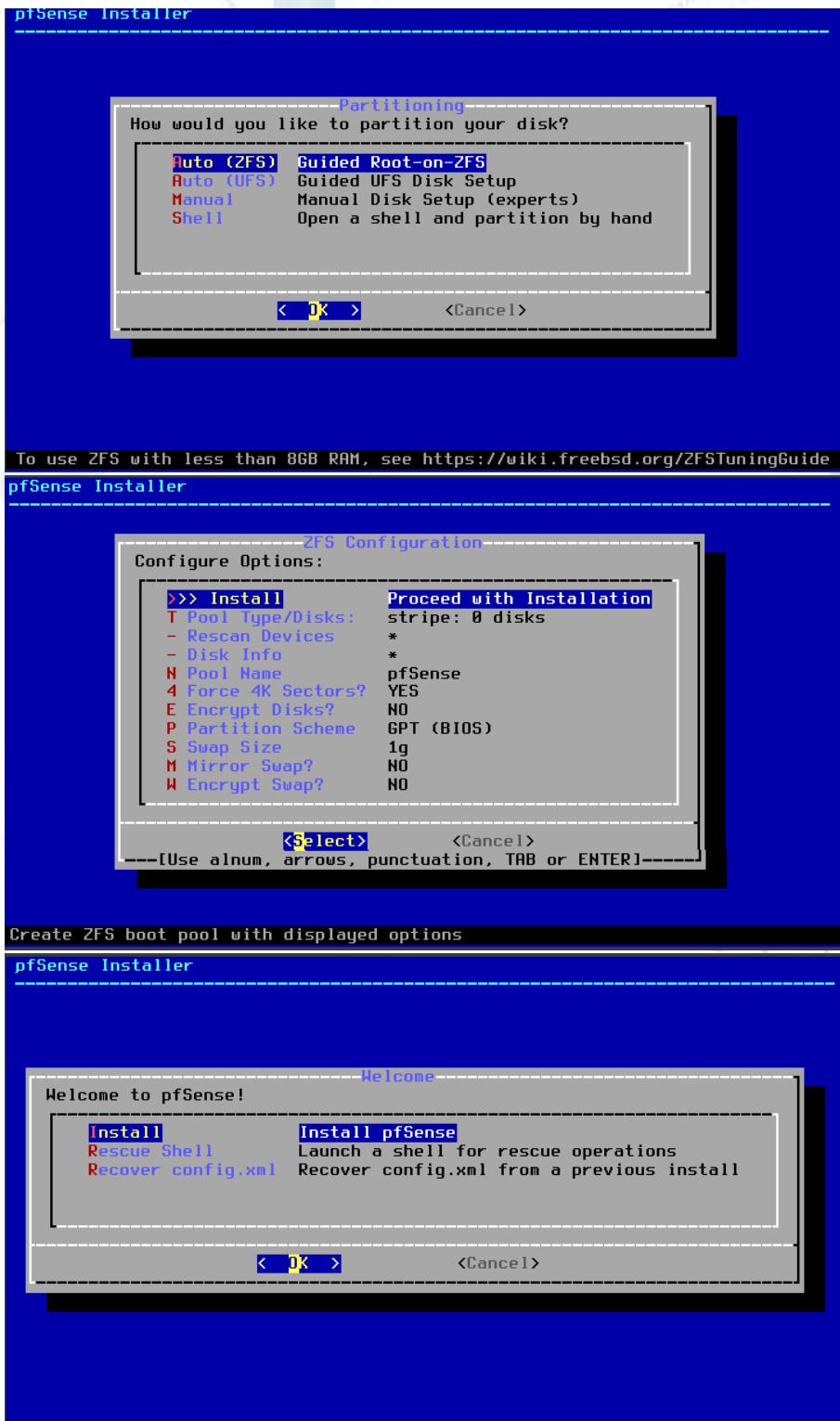
Creamos nuestra máquina Virtual con las siguientes configuraciones:

Nombre: UTM-01; Tipo: BSD; Subtype: FreeBSD; Versión: FreeBSD (64-bit)

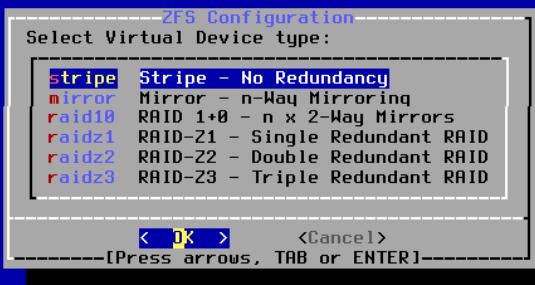


Lanzamos la maquina desde Virtual Box y comenzamos con las configuraciones.





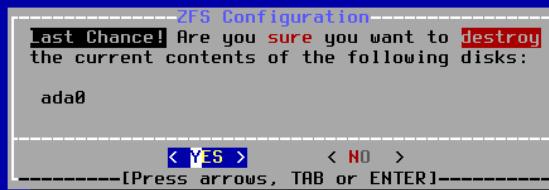
pfSense Installer



[1+ Disks] Striping provides maximum storage but no redundancy
pfSense Installer



pfSense Installer



pfSense Installer

-----|Checksum Verification|-----
base.txz [In Progress]

Verifying checksums of selected distributions.

-----|Overall Progress-----

0%

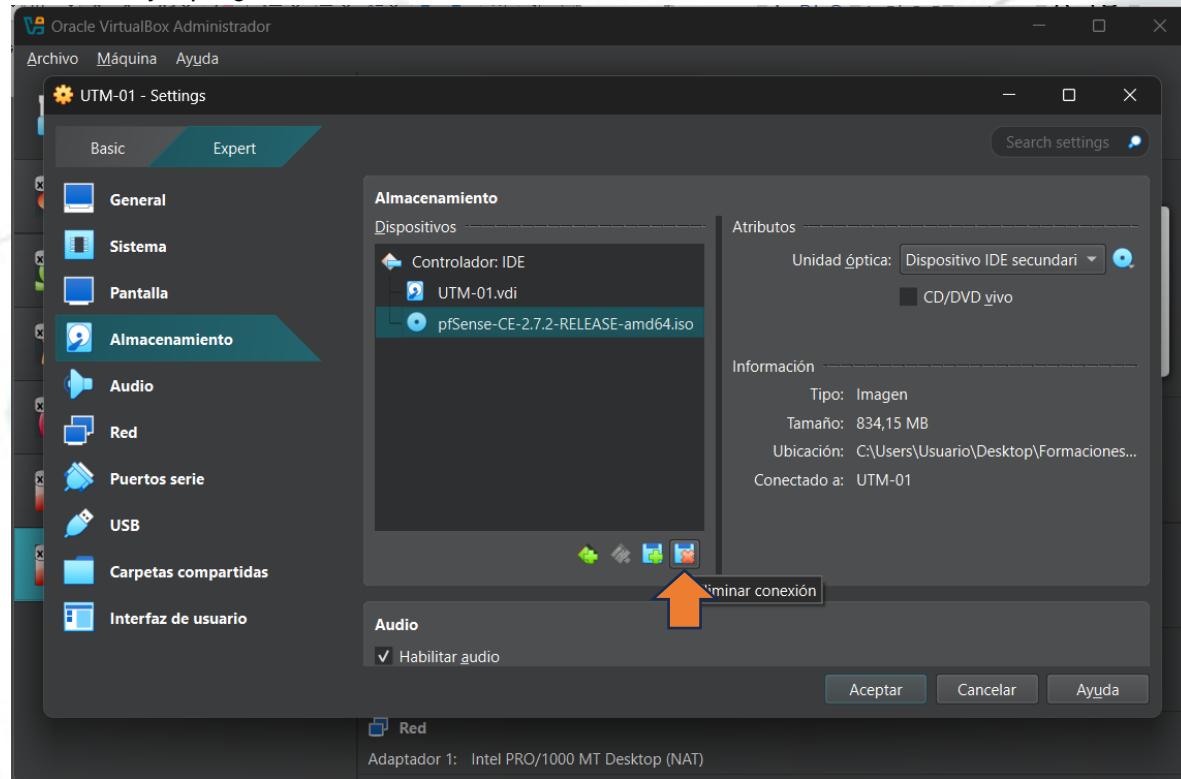
pfSense Installer

-----|Complete|-----

Installation of pfSense complete!
Would you like to reboot into the
installed system now?

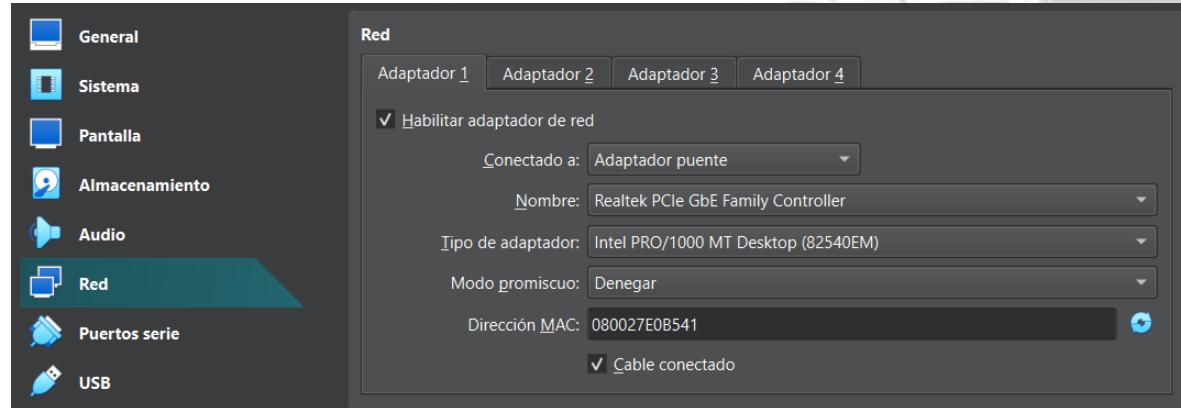
[Reboot] [Shell]

En este punto debemos apagar la máquina virtual y quitar el disco ISO desde las configuraciones de inicio, con este procedimiento evitamos que al lanzar nuevamente nuestro UTM-01 repita la instalación ya que generada.



Configuramos los adaptadores renombrando nuestras redes internas, nuevamente desde configuraciones en el apartado Red configuramos los parámetros.

Adaptador 1 | Conectado a: Adaptador puente | Nombre: default



Adaptador 2 | Conectado a: Red interna | Nombre: LAN

Red

Adaptador 1 Adaptador 2 **Adaptador 3** Adaptador 4

Habilitar adaptador de red

Conectado a: Red interna

Nombre: LAN

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Denegar

Dirección MAC: 08002728D34B

Cable conectado

Adaptador 3 | Conectado a: Red interna | Nombre: DMZ

Red

Adaptador 1 Adaptador 2 **Adaptador 3** Adaptador 4

Habilitar adaptador de red

Conectado a: Red interna

Nombre: DMZ

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Denegar

Dirección MAC: 080027AE25E1

Cable conectado

Adaptador 4 | Conectado a: Red interna | Nombre: DMZ2

Red

Adaptador 1 Adaptador 2 Adaptador 3 **Adaptador 4**

Habilitar adaptador de red

Conectado a: Red interna

Nombre: DMZ2

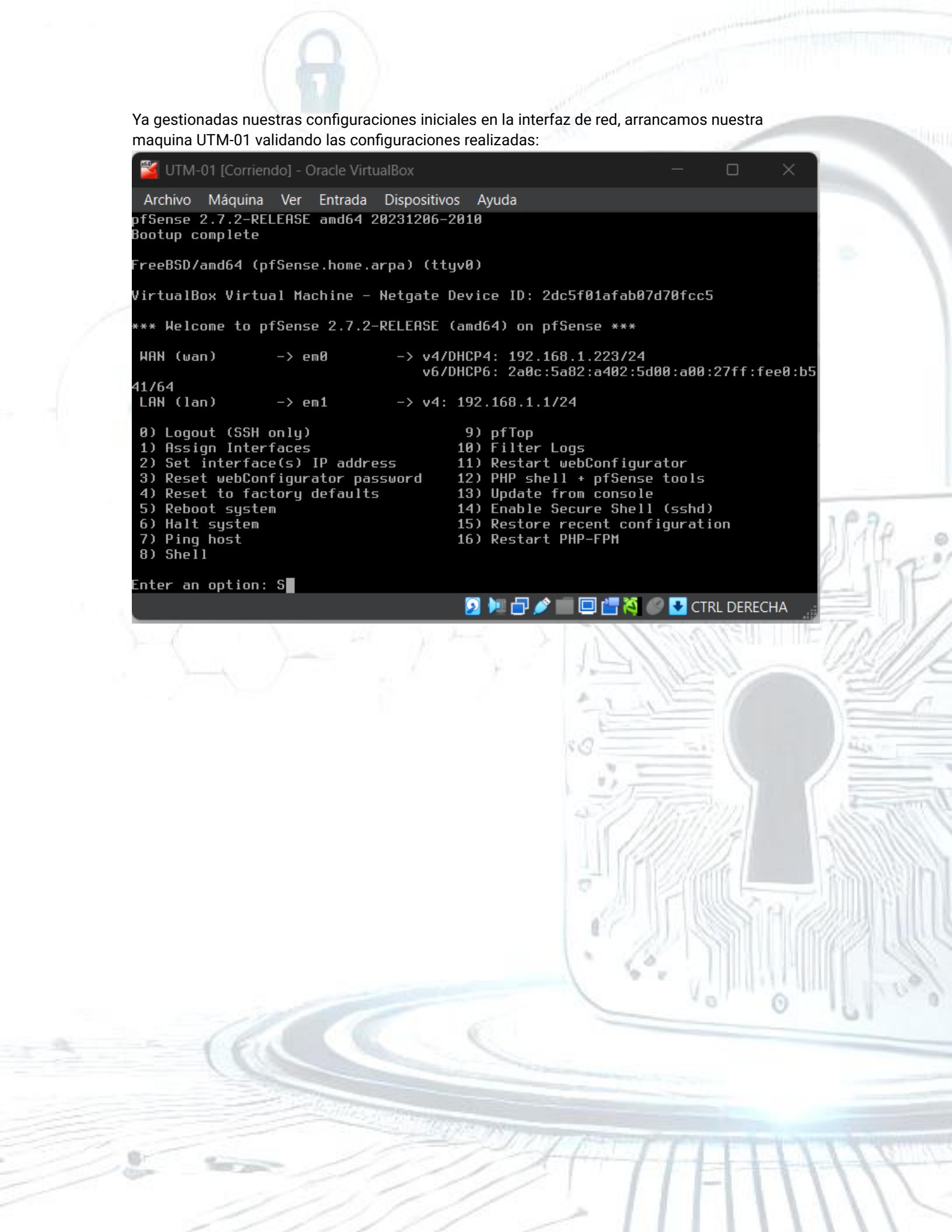
Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Denegar

Dirección MAC: 0800279B764E

Cable conectado

Ya gestionadas nuestras configuraciones iniciales en la interfaz de red, arrancamos nuestra maquina UTM-01 validando las configuraciones realizadas:



```
UTM-01 [Corriendo] - Oracle VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda  
pfSense 2.7.2-RELEASE amd64 20231206-2010  
Bootup complete  
  
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)  
  
VirtualBox Virtual Machine - Netgate Device ID: 2dc5f01afab07d70fcc5  
  
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.223/24  
                           v6/DHCP6: 2a0c:5a82:a402:5d00:a00:27ff:fee0:b5  
41/64  
LAN (lan)      -> em1      -> v4: 192.168.1.1/24  
  
0) Logout (SSH only)          9) pfTop  
1) Assign Interfaces          10) Filter Logs  
2) Set interface(s) IP address 11) Restart webConfigurator  
3) Reset webConfigurator password 12) PHP shell + pfSense tools  
4) Reset to factory defaults   13) Update from console  
5) Reboot system              14) Enable Secure Shell (sshd)  
6) Halt system                15) Restore recent configuration  
7) Ping host                  16) Restart PHP-FPM  
8) Shell  
  
Enter an option: S
```



Configuración pfSense.

Para realizar las configuraciones de cada red debemos acceder desde un navegador a la dirección IP de nuestra LAN, utilizaremos Kali para gestionarlo.

Nuestra dirección por defecto será 192.168.1.1

Debemos seleccionar “Aceptar el riesgo y continuar” para acceder al portal.

The screenshot shows a Firefox browser window with the URL <https://192.168.1.1>. A yellow warning icon is displayed, followed by the text: "Advertencia: riesgo potencial de seguridad a continuación". Below this, a message states: "Firefox ha detectado una posible amenaza de seguridad y no ha cargado 192.168.1.1. Si visita este sitio, los atacantes podrían intentar robar información como sus contraseñas, correos electrónicos o detalles de su tarjeta de crédito." There are two buttons at the bottom: "Retroceder (recomendado)" (Back (recommended)) and "Avanzado..." (Advanced...). A modal dialog box is overlaid, stating: "192.168.1.1 usa un certificado de seguridad no válido. No se confía en el certificado porque está autofirmado. Código de error: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT". It also has "Ver certificado" (View certificate) and "Retroceder (recomendado)" (Back (recommended)) buttons, along with an "Aceptar el riesgo y continuar" (Accept the risk and continue) button.

Las credenciales por defecto son “admin” para el usuario y contraseña.

The screenshot shows the pfSense Setup Wizard interface. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help, and a gear icon. A red warning box is present, stating: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title "Wizard / pfSense Setup /" is shown, along with a question mark icon. The main content area is titled "pfSense Setup" and contains the following text: "Welcome to pfSense® software! This wizard will provide guidance through the initial configuration of pfSense. The wizard may be stopped at any time by clicking the logo image at the top of the screen. pfSense® software is developed and maintained by Netgate®". There are "Learn more" and "» Next" buttons at the bottom.

Wizard / pfSense Setup / General Information

?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname

UTM

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain

keepcoding.local

Domain name for the firewall.

Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

127.0.0.1

Secondary DNS Server

1.1.1.1

Override DNS



Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Time Server Information

?

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname

2.pfsense.pool.ntp.org

Enter the hostname (FQDN) of the time server.

Timezone

Europe/Madrid

>> Next

Debemos liberar los bloqueos de WAN para evitar conflictos con nuestra red interna, ya que trabajaremos solo con tráfico interno.

This screenshot shows the pfSense configuration interface. The top section is titled 'RFC1918 Networks' and contains two sections: 'Block RFC1918 Private Networks' and 'Block bogon networks'. Under 'Block RFC1918 Private Networks', there is a checkbox labeled 'Block private networks from entering via WAN'. A note explains that this blocks traffic from IP addresses reserved for private networks (10/8, 172.16/12, 192.168/16) and loopback addresses (127/8). Under 'Block bogon networks', there is another checkbox labeled 'Block non-Internet routed networks from entering via WAN'. A note explains that this blocks traffic from IP addresses reserved by IANA or not yet assigned. At the bottom of the screen is a blue '» Next' button.

Cambiaremos la IP de LAN para evitar conflictos con la red de nuestro hogar.

This screenshot shows the 'Configure LAN Interface' step of the pfSense setup wizard. It is Step 5 of 9. The title bar says 'Wizard / pfSense Setup / Configure LAN Interface'. The main section is titled 'Configure LAN Interface' and contains instructions: 'On this screen the Local Area Network information will be configured.' Below this are fields for 'LAN IP Address' (set to 192.168.100.1) and 'Subnet Mask' (set to 24). A note below the IP address field says 'Type dhcp if this interface uses DHCP to obtain its IP address.' At the bottom is a blue '» Next' button.

Definimos una nueva clave de acceso, nuestras nuevas credenciales serán "user: admin | pass: 123456". Refrescamos la página, desconectamos y conectamos nuevamente la red.



Accedemos con la nueva IP asignadas y las credenciales correspondientes. De esta manera logramos acceso al portal para iniciar el resto de las configuraciones.

The screenshot shows the pfSense Status / Dashboard interface. On the left, there's a 'System Information' table with details like Name (UTM.keepcoding.local), User (admin@192.168.100.10), System (VirtualBox Virtual Machine, Netgate Device ID: 2dc5f01afab07d70fcc5), BIOS (Vendor: innotech GmbH, Version: VirtualBox, Release Date: Fri Dec 1 2006), Version (2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023, FreeBSD 14.0-CURRENT), CPU Type (AMD Ryzen 7 5700U with Radeon Graphics, AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No), Hardware crypto (Inactive), Kernel PTI (Disabled), MDS Mitigation (Inactive), Uptime (00 Hour 46 Minutes 27 Seconds), Current date/time (Sun Jan 12 11:57:57 CET 2025), and a note that the system is on the latest version. On the right, there's a 'Netgate Services And Support' section with a 'Contract type' set to 'Community Support' (Community Support Only). Below it is a 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES' section with links to upgrade support, community resources, Netgate Global Support FAQ, official pfSense training, professional services, and the Netgate website. A note at the bottom of this section states that to purchase a Netgate Global TAC Support subscription, one must have their Netgate Device ID (NDI) from their firewall.

Configuramos el servidor de DNS en nuestro pfSense. Para ello accedemos al apartado *ServicesDNS / ResolverGeneral / Settings*.

Quitamos el check del apartado “Enable DNSSEC Support” y colocamos el check en “Enable Forwarding Mode”.

The screenshot shows the 'ServicesDNS / ResolverGeneral / Settings' page. Under 'DNSSEC', the 'Enable DNSSEC Support' checkbox is unchecked. Under 'Python Module', the 'Enable Python Module' checkbox is unchecked. Under 'DNS Query Forwarding', the 'Enable Forwarding Mode' checkbox is checked. A note below explains that if this option is set, DNS queries will be forwarded to upstream DNS servers defined under 'System > General Setup' or via dynamic interfaces like DHCP, PPP, or OpenVPN if DNS Server Override is enabled.

IMPORTANTE “En todas las modificaciones que gestionemos, debemos aplicar los cambios desde el siguiente botón:

Apply Changes

Configuraremos pfSense para que asigne IP dinámicos por cada Red generada. Usaremos datos conocidos para la configuración:

LAN: 192.168.100.1/24 Rango DHCP: 192.168.100.100 - 192.168.100.200

DMZ: 192.168.200.1/24 Rango DHCP: 192.168.200.100 - 192.168.200.150

DMZ2: 192.168.250.1/24 Rango DHCP: 192.168.250.100 - 192.168.250.150

Habilitamos todas las interfaces a utilizar desde el apartado *Interfaces / Interface Assignments*.

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Interfaces / Interface Assignments

Interface has been added.

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	em0 (08:00:27:e0:b5:41)
LAN	em1 (08:00:27:28:d3:4b)
OPT1	em2 (08:00:27:ae:25:e1)
OPT2	em3 (08:00:27:9b:76:4e)

Save

Desde el apartado *Services / DHCP / Server LAN* realizaremos la configuración de LAN con los parámetros antes mencionados:

Primary Address Pool

Subnet 192.168.100.0/24

Subnet Range 192.168.100.1 - 192.168.100.254

Address Pool Range 192.168.100.100 To 192.168.100.200

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools + Add Address Pool

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	192.168.100.1
	1.1.1.1
	8.8.8.8
	DNS Server 4

Other DHCP Options

Gateway	192.168.100.1
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.	

Desde el apartado *Interfaces / OPT1 (em2)* realizaremos las configuraciones para la red DMZ

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	DMZ
Enter a description (name) for the interface here.	
IPv4 Configuration Type	Static IPv4

Static IPv4 Configuration

IPv4 Address	192.168.200.1	/ 24
IPv4 Upstream gateway	None	+ Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.		

Aplicamos los cambios correspondientes en el apartado *Interfaces / OPT2 (em3)* para Red DMZ2

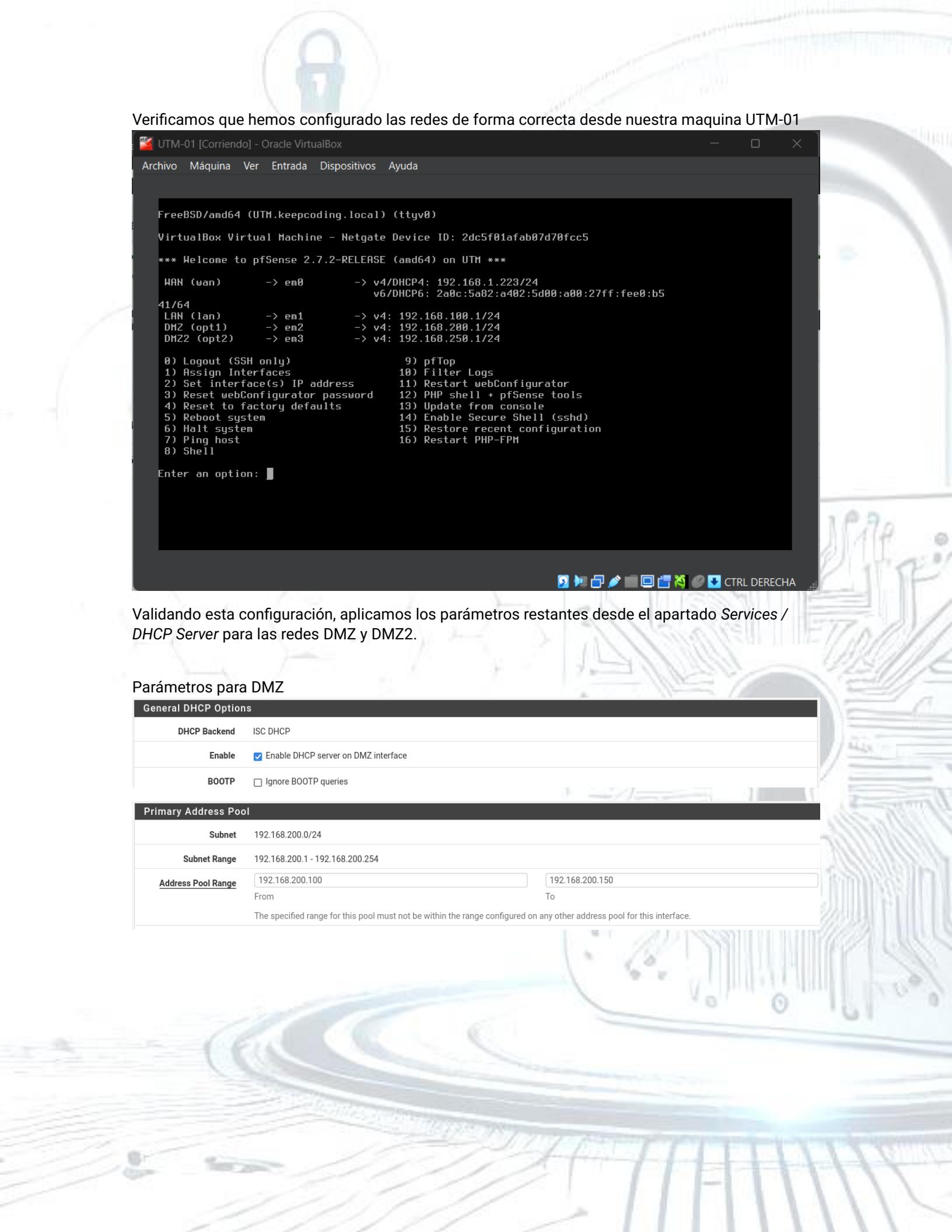
General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	DMZ2
Enter a description (name) for the interface here.	
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None

Static IPv4 Configuration

IPv4 Address	192.168.250.1	/ 24
IPv4 Upstream gateway	None	+ Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface . Gateways can be managed by clicking here .		

Verificamos que hemos configurado las redes de forma correcta desde nuestra maquina UTM-01



```
UTM-01 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

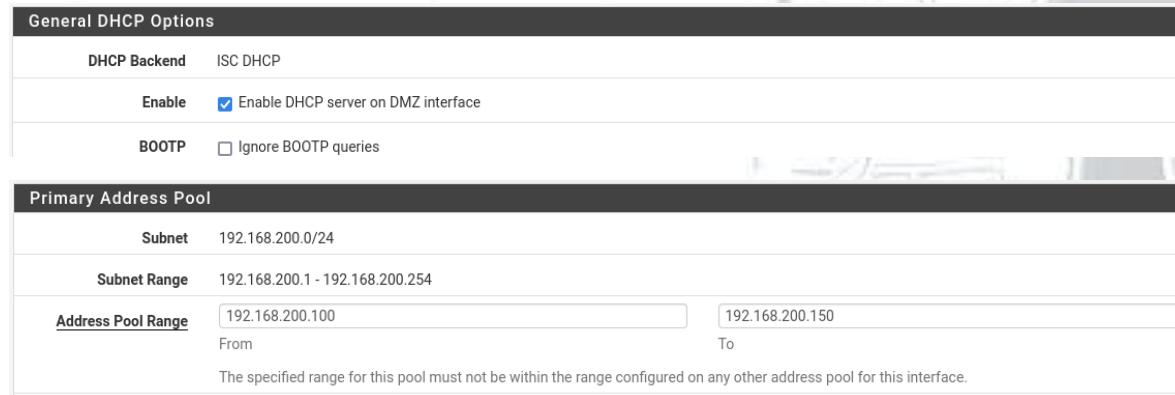
FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 2dc5f01afab07d70fcc5
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM ***
WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.223/24
                           v6/DHCP6: 2a0c:5a82:a402:5d00:a00:27ff:fee0:b5
41/64
LAN (lan)      -> em1          -> v4: 192.168.100.1/24
DMZ (opt1)     -> em2          -> v4: 192.168.200.1/24
DMZ2 (opt2)    -> em3          -> v4: 192.168.250.1/24
8) Logout (SSH only)      9) pfTop
1) Assign Interfaces       10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system           14) Enable Secure Shell (sshd)
6) Halt system             15) Restore recent configuration
7) Ping host               16) Restart PHP-FPM
8) Shell

Enter an option: ■
```

CTRL DERECHA

Validando esta configuración, aplicamos los parámetros restantes desde el apartado Services / DHCP Server para las redes DMZ y DMZ2.

Parámetros para DMZ



The screenshot shows the pfSense configuration interface for the DMZ network. It includes sections for 'General DHCP Options' (with 'Enable' checked) and 'Primary Address Pool' (with Subnet set to 192.168.200.0/24 and a range of 192.168.200.1 - 192.168.200.254). A note at the bottom states: 'The specified range for this pool must not be within the range configured on any other address pool for this interface.'

Server Options

WINS Servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="192.168.200.1"/>
	<input type="text" value="1.1.1.1"/>
	<input type="text" value="8.8.8.8"/>
	<input type="text" value="DNS Server 4"/>

Other DHCP Options

Gateway	<input type="text" value="192.168.200.1"/>
<p>The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.</p>	

Parámetros para DMZ2

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on DMZ2 interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries

Primary Address Pool

Subnet	192.168.250.0/24
Subnet Range	192.168.250.1 - 192.168.250.254
Address Pool Range	<input type="text" value="192.168.250.100"/> From <input type="text" value="192.168.250.150"/> To
<p>The specified range for this pool must not be within the range configured on any other address pool for this interface.</p>	

Server Options

WINS Servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="192.168.250.1"/>
	<input type="text" value="1.1.1.1"/>
	<input type="text" value="8.8.8.8"/>

Other DHCP Options

Gateway	<input type="text" value="192.168.250.1"/>
<p>The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.</p>	
Domain Name	<input type="text" value="keencloud.local"/>

Definimos las normas de Firewall para cada Red creada.

Previamente a esta configuración, asignaremos un alias para simplificar los parámetros en las normas de firewall. Desde el apartado *Firewall / Aliases / Ports* agregamos el alias “Web” con los puertos 443 y 80 para configurar los accesos a internet.

Firewall / Aliases / Edit

Properties	
Name	<input type="text" value="Web"/> The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	<input type="text" value="Puertos para traficos Web"/> A description may be entered here for administrative reference (not parsed).
Type	<input type="text" value="Port(s)"/>
Port(s)	
Hint	Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.
Port	<input type="text" value="80"/> http <input type="button" value="Delete"/>
	<input type="text" value="443"/> https <input type="button" value="Delete"/>
<input type="button" value="Save"/> <input type="button" value="Add Port"/>	

Utilizaremos las configuraciones por default de la Red LAN, por lo que aplicaremos en principio, las configuraciones básicas para las Redes DMZ y DMZ2.

Desde el apartado *Firewall/Rules/DMZ* asignamos los parámetros en la Red DMZ.

Aplicamos las normas para el acceso a internet.

Edit Firewall Rule

Action	<input type="text" value="Pass"/> Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="text" value="DMZ"/> Choose the interface from which packets must come to match this rule.
Address Family	<input type="text" value="IPv4"/> Select the Internet Protocol version this rule applies to.
Protocol	<input type="text" value="TCP"/> Choose which IP protocol this rule should match.

Source

<u>Source</u>	<input type="checkbox"/> Invert match	Any	Source Address	/	<input type="button"/>
Display Advanced					
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.					

Destination

<u>Destination</u>	<input type="checkbox"/> Invert match	Any	Destination Address	/	<input type="button"/>
Destination Port Range	(other)	Web	(other)	Web	Custom
From	Custom	To	Custom		
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.					

Extra Options

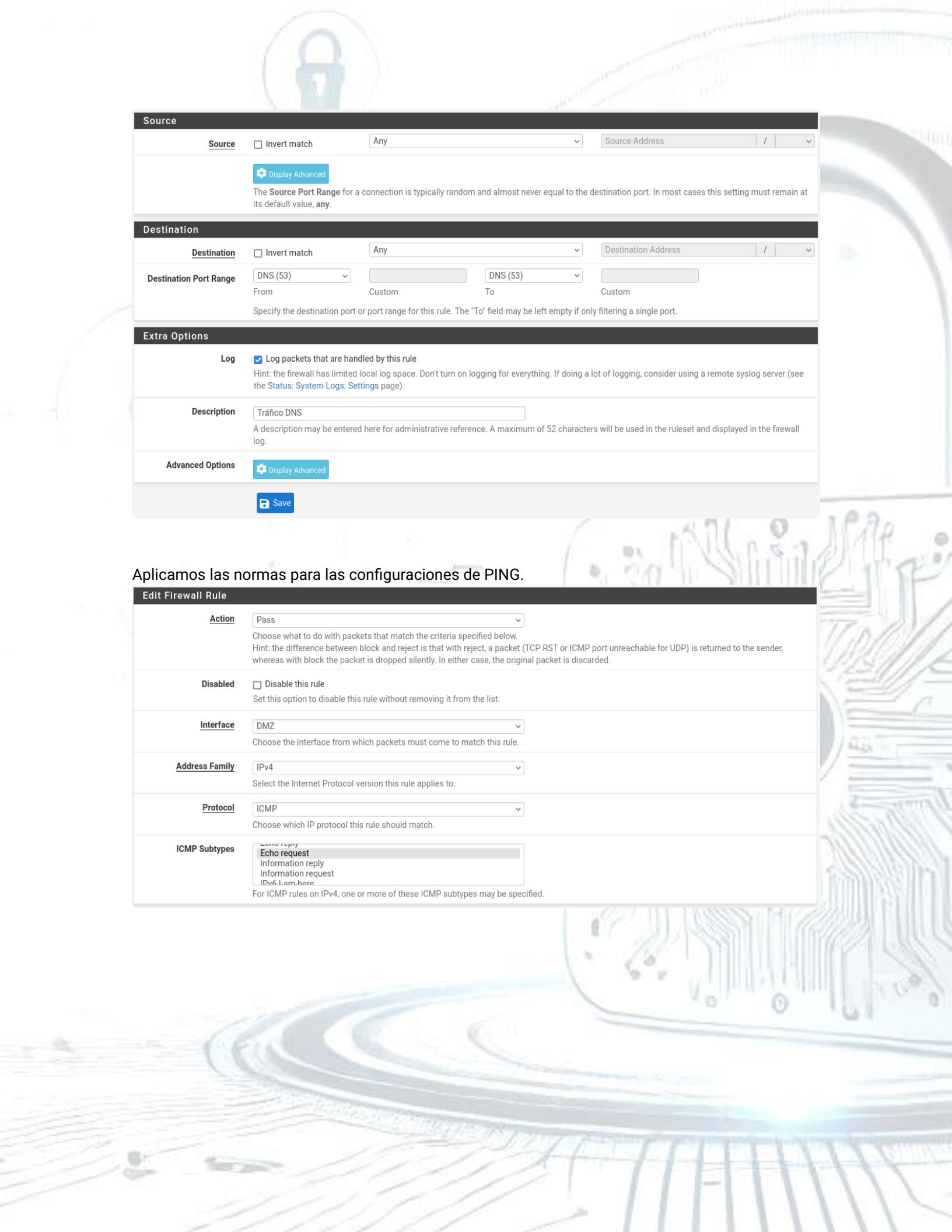
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Tráfico Web
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	Display Advanced

Save

Aplicamos las normas para las configuraciones de DNS.

Edit Firewall Rule

Action	Pass	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
Interface	DMZ	Choose the interface from which packets must come to match this rule.
Address Family	IPv4	Select the Internet Protocol version this rule applies to.
Protocol	UDP	Choose which IP protocol this rule should match.



Source

Source Invert match /

[Display Advanced](#)

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match /

Destination Port Range From To To

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

Aplicamos las normas para las configuraciones de PING.

Edit Firewall Rule

Action
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface
Choose the interface from which packets must come to match this rule.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

ICMP Subtypes Echo reply
 Echo request
 Information reply
 Information request
 IPv6 I am here

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source	<input type="checkbox"/> Invert match	Any	Source Address	/	<input type="button"/>
---------------	---------------------------------------	-----	----------------	---	------------------------

Destination

Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	<input type="button"/>
--------------------	---------------------------------------	-----	---------------------	---	------------------------

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Norma Ping
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	<input type="button"/> Display Advanced

Save

Las reglas definidas para la Red DMZ son las siguientes:

Floating	WAN	LAN	DMZ	DMZ2							
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 ICMP echoreq	*	*	*	*	*	none		Norma Ping	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		Tráfico DNS	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	*	Web	*	none		Tráfico Web	

Replicamos las mismas configuraciones sobre la Red DMZ2 antes de comenzar a gestionar las restricciones sobre la Red DMZ quedando de la siguiente manera:

Floating	WAN	LAN	DMZ	DMZ2							
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 ICMP echoreq	*	*	*	*	*	none		Norma Ping	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		Tráfico DNS	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	*	Web	*	none		Tráfico Web	

Configuramos una IP estática sobre la Red DMZ para hace accesible desde el exterior el Honeypot. Asignaremos el IP "192.168.200.99" desde el apartado Services / DHCP Server / DMZ / Static Mapping / Edit.

Static DHCP Mapping on DMZ

DHCP Backend	ISC DHCP	
MAC Address	08:00:27:ad:25:87	<input type="button" value="Copy My MAC"/>
MAC address of the client to match (6 hex octets separated by colons).		
Client Identifier		
An optional identifier to match based on the value sent by the client (RFC 2132).		
IP Address	192.168.200.99	IPv4 address to assign this client.
Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool. The same IP address may be assigned to multiple mappings.		
ARP Table Static Entry	<input checked="" type="checkbox"/> Create an ARP Table Static Entry for this MAC & IP Address pair.	
Hostname	kali	
Name of the client host without the domain part.		
Description		
A description for administrative reference (not parsed).		

DHCP Static Mappings

Static ARP	MAC address	IP address	Hostname	Description
✓	08:00:27:ad:25:87	192.168.200.99	kali	

[+ Add Static Mapping](#)

Evidenciamos la configuración desde Kali conectado a la Red DMZ en el terminal.

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
        inet 192.168.200.99/24 brd 192.168.200.255 scope global dynamic noprefixroute eth0
            valid_lft 7177sec preferred_lft 7177sec
            inet6 fe80::f50a:c692:d036:dc9a/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:95:c7:58:87 brd ff:ff:ff:ff:ff:ff
        inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
            valid_lft forever preferred_lft forever
```

Restricciones de Red.

Configuraremos nuestro Firewall desde pfSense para que DMZ no tenga acceso al resto de las redes.

Utilizaremos los siguientes parámetros para configurar cada Red.

Edit Firewall Rule

Action	Block
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	Any
Choose which IP protocol this rule should match.	
Source	
Source	<input type="checkbox"/> Invert match
LAN subnets	
Source Address /	
Destination	
Destination	<input type="checkbox"/> Invert match
DMZ subnets	
Destination Address /	
Extra Options	
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Restringir conexión a DMZ
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	Display Advanced
Rule Information	
Tracking ID	1737297603
Created	1/19/25 15:40:03 by admin@192.168.100.100 (Local Database)
Updated	1/19/25 15:40:03 by admin@192.168.100.100 (Local Database)
Save	

Quedando configurados de la siguiente manera:

Floating WAN LAN **DMZ** DMZ2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/1.53 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	Edit
<input type="checkbox"/>	0/4 KiB	IPv4	*	LAN subnets	*	DMZ subnets	*	*	none	Restringir conexión a DMZ	Edit Delete Copy Reset X
<input checked="" type="checkbox"/>	2/7.15 MiB	IPv4	*	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	Edit Delete Copy Reset X
<input checked="" type="checkbox"/>	0/0 B	IPv6	*	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	Edit Delete Copy Reset X

Floating WAN LAN **DMZ** DMZ2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>		0/588 B	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none	Restricción conexión a DMZ2	
<input type="checkbox"/>		0/5 KiB	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none	Restricción conexión a LAN	
<input checked="" type="checkbox"/>		0/4 KiB	IPv4 ICMP echoreq	*	*	*	*	*	none	Norma Ping	
<input checked="" type="checkbox"/>		14/368 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none	Tráfico DNS	
<input checked="" type="checkbox"/>		24/37.50 MiB	IPv4 TCP	*	*	*	Web	*	none	Tráfico Web	

Floating WAN LAN **DMZ** DMZ2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>		0/1 KiB	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	*	none	Restricción conexión a DMZ	
<input checked="" type="checkbox"/>		0/8 KiB	IPv4 ICMP echoreq	*	*	*	*	*	none	Norma Ping	
<input checked="" type="checkbox"/>		0/50 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none	Tráfico DNS	
<input checked="" type="checkbox"/>		17/827 KiB	IPv4 TCP	*	*	*	Web	*	none	Tráfico Web	

LAN no podrá conectarse con DMZ, pero si con WAN y DMZ2

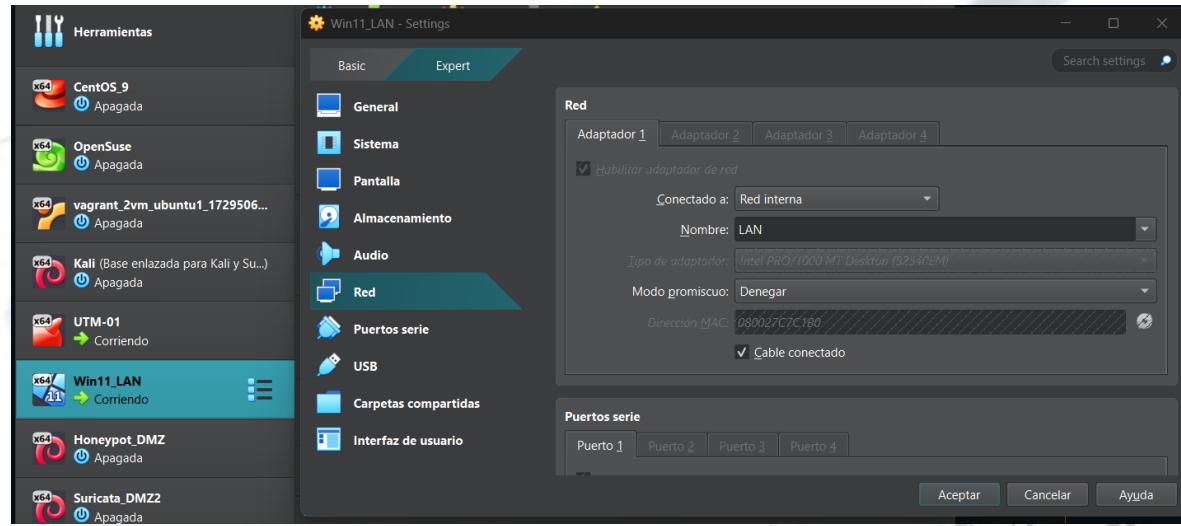
DMZ2 no podrá conectarse con DMZ, pero si con LAN y WAN

DMZ no podrá conectarse con LAN y WAN

WAN podrá conectarse con LAN, DMZ y DMZ2

2. En la red LAN debe haber un equipo Windows 11 que envíe logs al servidor de Elastic.

Para generar la conexión dentro de nuestro UTM-01, instalaremos una ISO de Wind11 en nuestra Virtual Box, dejando las siguientes configuraciones.

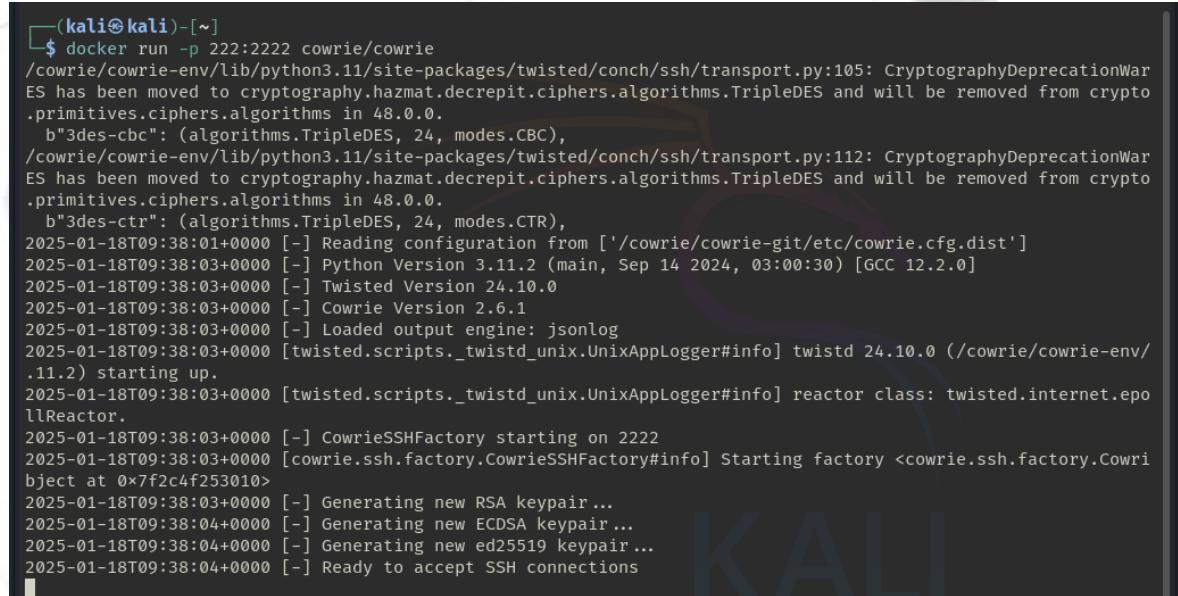


3. En la red DMZ debe haber un honeypot que envíe los logs al servidor de Elastic.

1. Este honeypot no debe tener acceso a ninguna red interna (LAN, DMZ2...) y debe ser accesible desde el exterior (red WAN) en ambos sentidos.

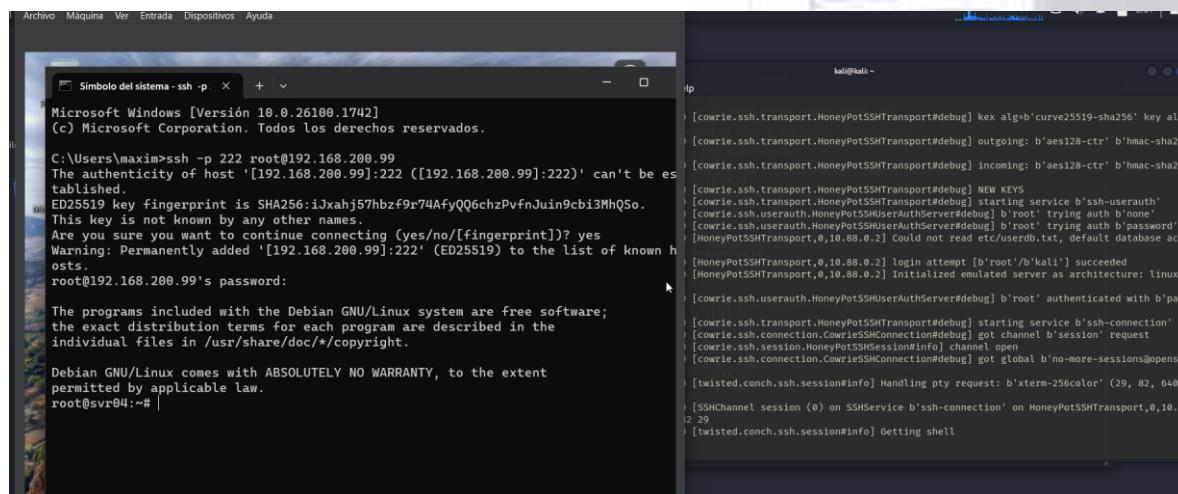
En este punto utilizaremos Cowrie como Honeypot por su facilidad de configuración. Desde los repositorios Docker con el siguiente comando:

```
docker run -p 222:2222 cowrie/cowrie
```



```
(kali㉿kali)-[~]
$ docker run -p 222:2222 cowrie/cowrie
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:105: CryptographyDeprecationWarning: has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.primitives.ciphers.algorithms in 48.0.0.
    b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:112: CryptographyDeprecationWarning: has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.primitives.ciphers.algorithms in 48.0.0.
    b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
2025-01-18T09:38:01+0000 [-] Reading configuration from ['/cowrie/cowrie-git/etc/cowrie.cfg.dist']
2025-01-18T09:38:03+0000 [-] Python Version 3.11.2 (main, Sep 14 2024, 03:00:30) [GCC 12.2.0]
2025-01-18T09:38:03+0000 [-] Twisted Version 24.10.0
2025-01-18T09:38:03+0000 [-] Cowrie Version 2.6.1
2025-01-18T09:38:03+0000 [-] Loaded output engine: jsonlog
2025-01-18T09:38:03+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 24.10.0 (/cowrie/cowrie-env/.11.2) starting up.
2025-01-18T09:38:03+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet. epollReactor.
2025-01-18T09:38:03+0000 [-] CowrieSSHFactory starting on 2222
2025-01-18T09:38:03+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f2c4f253010>
2025-01-18T09:38:03+0000 [-] Generating new RSA keypair ...
2025-01-18T09:38:04+0000 [-] Generating new ECDSA keypair ...
2025-01-18T09:38:04+0000 [-] Generating new ed25519 keypair ...
2025-01-18T09:38:04+0000 [-] Ready to accept SSH connections
```

Para validar el funcionamiento correcto, conectaremos nuestro Wind11 con el protocolo SSH usando el siguiente comando `ssh -p 222 root@192.168.200.99` (Se asignó como IP estática previamente)



```
Archivo Máquina Ver Entrada Dispositivos Ayuda

Microsoft Windows [Versión 10.0.26100.1742]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\maxim>ssh -p 222 root@192.168.200.99
The authenticity of host '[192.168.200.99]:222 ([192.168.200.99]:222)' can't be established.
ED25519 key fingerprint is SHA256:ijXahj57hbzf9r74AfYQQ6chzPvfJuin9cbi3MhQSo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.200.99]:222' (ED25519) to the list of known hosts.
root@192.168.200.99's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~#
```

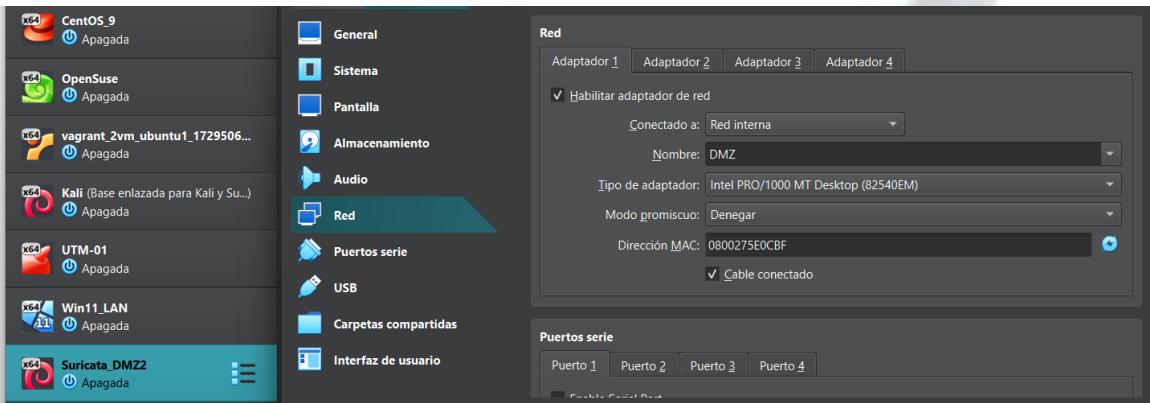
```
kali㉿kali:~
```

```
[cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key algorithm selected
[cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-sha256'
[cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha256'
[cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEY
[cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
[cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'mono'
[cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
[HoneyPotSSHTransport,0,10.88.0.2] Could not read etc/userdb.txt, default database used
[HoneyPotSSHTransport,0,10.88.0.2] login attempt [b'root'/b'kali'] succeeded
[HoneyPotSSHTransport,0,10.88.0.2] initialized emulated server as architecture: linux
[cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
[cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
[cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
[cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions' opens
[twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (29, 82, 648)
[SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,0,10.88.0.2]
[SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,0,10.88.0.2]
[SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,0,10.88.0.2]
[twisted.conch.ssh.session#info] Getting shell
```

4. En la red DMZ2 debe haber otra fuente diferente de logs a las dos mencionadas anteriormente.

Se propone Suricata o Apache Server como posibles fuentes, pero se deja a elección del alumno.

Creamos nuestra máquina virtual denominada "Suricata_DMZ2", para generar nuestro log desde Suricata. Configuramos tipo de Red Interna / DMZ2.



Dentro de la máquina actualizaremos los paquetes e instalaremos Suricata con los siguientes comandos:

```
sudo apt update && sudo apt install suricata
```

```
(kali㉿kali)-[~]
$ suricata -V

This is Suricata version 7.0.8 RELEASE
```

Antes de la lanzar la herramienta vamos a generar las reglas de monitoreo/log. Vamos a seguir el orden de los siguientes comandos en el terminal de la máquina virtual.

`sudo -s` para gestionar con permisos de Root.

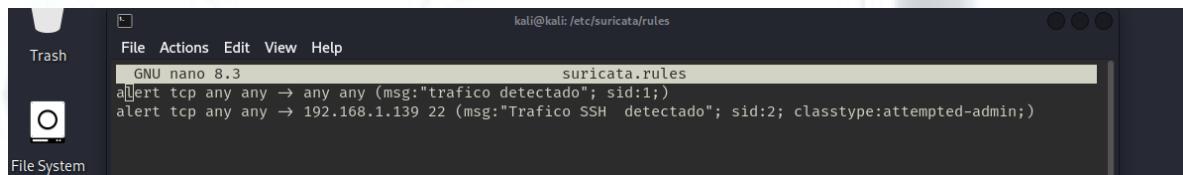
`cd /etc/suricata/rules` para movernos al directorio de Reglas.

`touch suricata.rules` para generar el archivo donde definiremos los parámetros.

Asignaremos las siguientes normas:

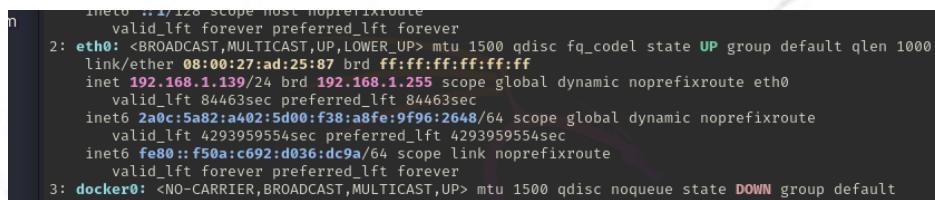
```
alert tcp any any -> any any (msg:"trafico detectado"; sid:1;)
```

```
alert tcp any any -> 192.168.1.65 22 (msg:"Trafico SSH detectado"; sid:2; classtype:attempted-admin;)
```



```
File System
File   Actions   Edit   View   Help
GNU nano 8.3          suricata.rules
alert tcp any any -> any any (msg:"trafico detectado"; sid:1;)
alert tcp any any -> 192.168.1.65 22 (msg:"Trafico SSH detectado"; sid:2; classtype:attempted-admin;)
```

Considerar que la segunda regla de identificara el IP de nuestra máquina virtual, lo consultamos en un nuevo terminal con el comando `ip a`.



```
inet ... scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.139/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 84463sec preferred_lft 84463sec
        inet6 2a0c:5ab2:a402:5d00:f38:8fe:9f96:2648/64 scope global dynamic noprefixroute
            valid_lft 4293959554sec preferred_lft 4293959554sec
        inet6 fe80::f50a:c692:d036:dc9a/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
```

Nos movemos al directorio `/etc/suricata` para configurar el archivo `suricata.yaml` de la siguiente manera:

```
# This parameter has no effect if auto-config is disabled.
#
hashmode: hash5tuplesorted

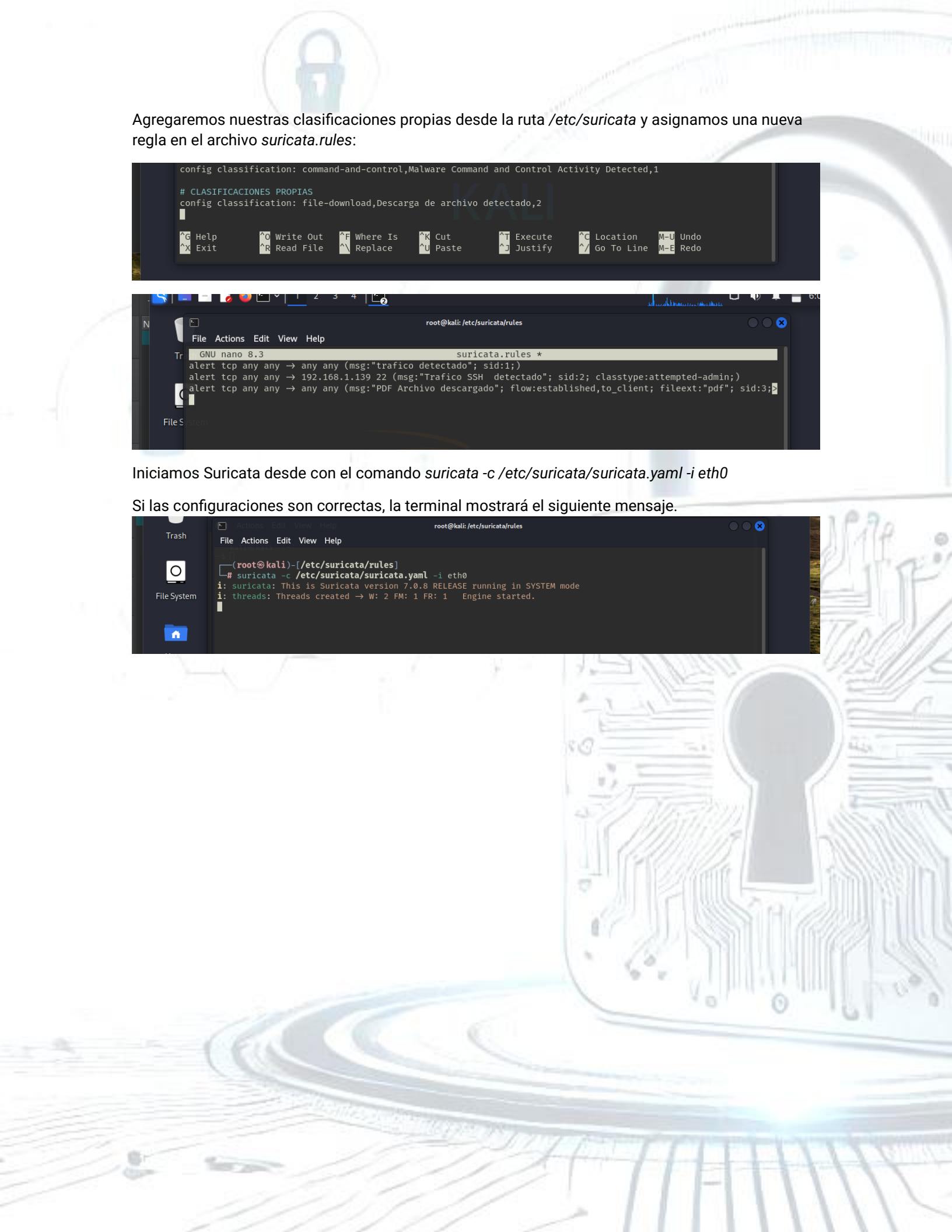
##
## Configure Suricata to load Suricata-Update managed rules.
##

#default-rule-path: /var/lib/suricata/rules
default-rule-path: /etc/suricata/rules

rule-files:
  - suricata.rules
```

Asignamos la ruta `default-rule-path: /etc/suricata/rules` y comentamos la siguiente fila `#default-rule-path: /var/lib/suricata/rules`. Tendremos este acceso como backup ante conflictos futuros.

Agregaremos nuestras clasificaciones propias desde la ruta `/etc/suricata` y asignamos una nueva regla en el archivo `suricata.rules`:



The background of the slide features a watermark of a padlock and a circuit board.

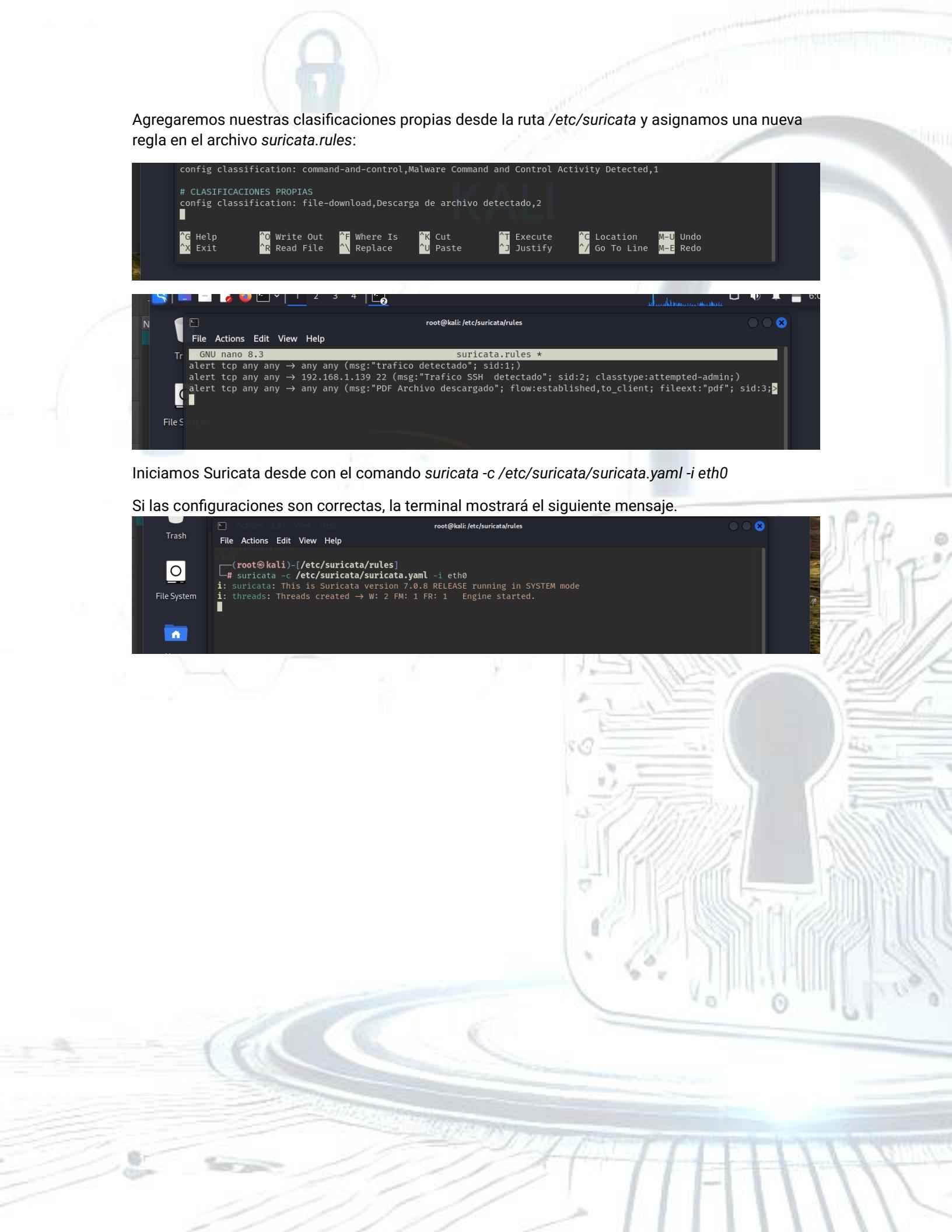
```
config classification: command-and-control,Malware Command and Control Activity Detected,1
# CLASIFICACIONES PROPIAS
config classification: file-download,Descarga de archivo detectado,2
|
^G Help      ^O Write Out   ^F Where Is    ^K Cut        ^T Execute   ^C Location   M-U Undo
^X Exit      ^R Read File   ^L Replace     ^U Paste     ^J Justify   ^V Go To Line M-E Redo
```



```
File Actions Edit View Help
root@kali:/etc/suricata/rules
Tr GNU nano 8.3          suricata.rules *
alert tcp any any → any any (msg:"trafico detectado"; sid:1;)
alert tcp any any → 192.168.1.139 22 (msg:"Trafico SSH detectado"; sid:2; classtype:attempted-admin;)
alert tcp any any → any any (msg:"PDF Archivo descargado"; flow:established,to_client; fileext:"pdf"; sid:3;)
```

Iniciamos Suricata desde con el comando `suricata -c /etc/suricata/suricata.yaml -i eth0`

Si las configuraciones son correctas, la terminal mostrará el siguiente mensaje.



The background of the slide features a watermark of a padlock and a circuit board.

```
File Actions Edit View Help
root@kali:/etc/suricata/rules
[root@kali]-(/etc/suricata/rules]
# suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode.
i: threads: Threads created → W: 2 FM: 1 FR: 1 Engine started.
```

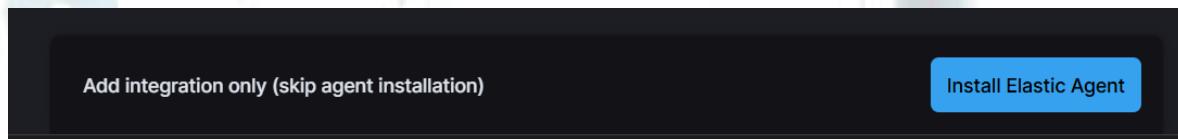
5. El servidor de Elastic debe recibir, almacenar y poder visualizar los logs del honeypot, el Windows 11 y la fuente elegida ubicada en la DMZ2.

Realizamos las configuraciones de Elastic para enlazar cada máquina virtual y gestionar los logs de cada una.

Desde <https://www.elastic.co/es/cloud> creamos nuestra cuenta con los datos solicitados, utilizaremos un usuario temporal para la práctica.

Una vez creada la cuenta comenzamos a configurar desde el apartado Assets > Agent policies > Create agent policy. *Evidenciamos las configuraciones para "Suricata/Linux" y replicaremos las configuraciones básicas para el resto de lokalis Agent.*

Para generar la integración utilizamos el apartado Assets > Agent policies > Add integration > Add Suricata. Pinchamos el botón emergente para acceder al enrolamiento.



Seguimos las instrucciones para Linux Tar

1 **Install Elastic Agent on your host**

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our [installation docs](#).

⚠ Root privileges required

This agent policy contains the following integrations that require Elastic Agents to have root privileges. To ensure that all data required by the integrations can be collected, enroll the agents using an account with root privileges. For more information, see the [Fleet and Elastic Agent Guide](#).

- System

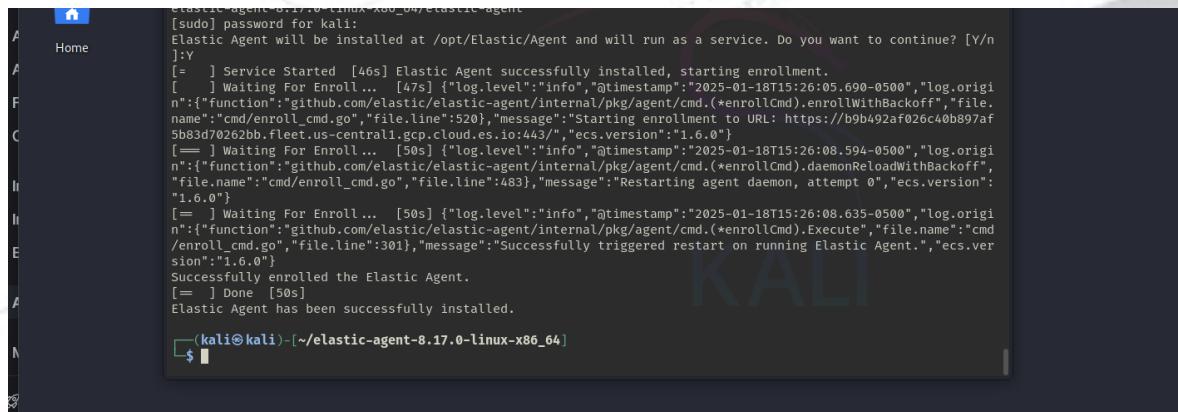
To install Elastic Agent without root privileges, add the `--unprivileged` flag to the `elastic-agent install` command below. For more information, see the [Fleet and Elastic Agent Guide](#).

Linux Tar Mac Windows RPM DEB Kubernetes

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-tar.xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz  
cd elastic-agent-8.17.0-linux-x86_64  
sudo ./elastic-agent install --url=https://b9b492af026c40b897af5b83d70262bb.fleet.us-central1.elastic-cloud.com:443
```

Copy to clipboard

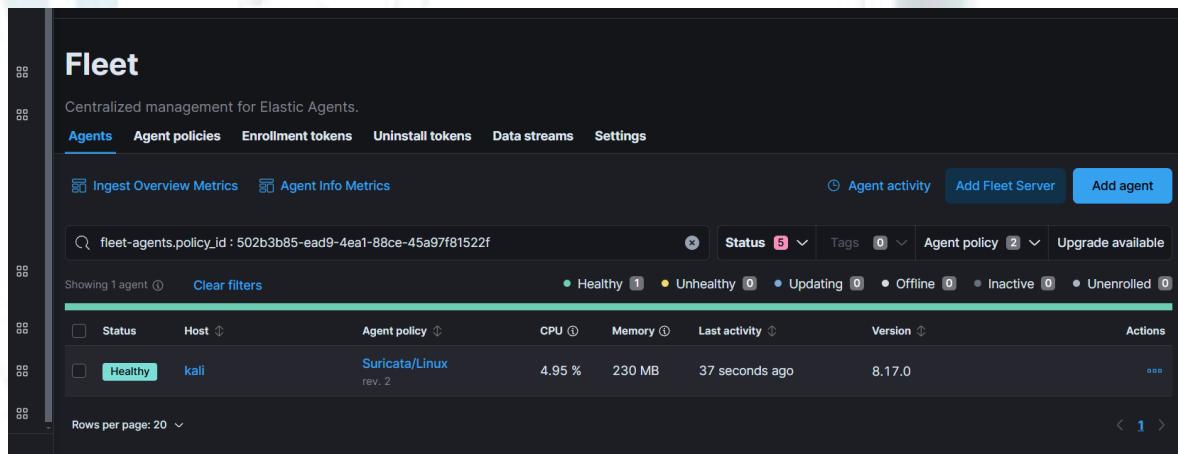
Desde nuestra terminal Suricata lanzamos el comando.



```
[sudo] password for kali:
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [y/n]
]:Y
[= ] Service Started [46s] Elastic Agent successfully installed, starting enrollment.
[= ] Waiting For Enroll... [47s] {"log.level": "info", "@timestamp": "2025-01-18T15:26:05.690-0500", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": 520}, "message": "Starting enrollment to URL: https://b9b492af026c40bb97af5bb3d70262bb.fleet.us-central1.gcp.cloud.es.io:443/", "ecs.version": "1.6.0"}
[= ] Waiting For Enroll... [50s] {"log.level": "info", "@timestamp": "2025-01-18T15:26:08.594-0500", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": 483}, "message": "Restarting agent daemon, attempt 0", "ecs.version": "1.6.0"}
[= ] Waiting For Enroll... [50s] {"log.level": "info", "@timestamp": "2025-01-18T15:26:08.635-0500", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).Execute", "file.name": "cmd/enroll_cmd.go", "file.line": 301}, "message": "Successfully triggered restart on running Elastic Agent.", "ecs.version": "1.6.0"}
Successfully enrolled the Elastic Agent.
[= ] Done [50s]
Elastic Agent has been successfully installed.

(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
```

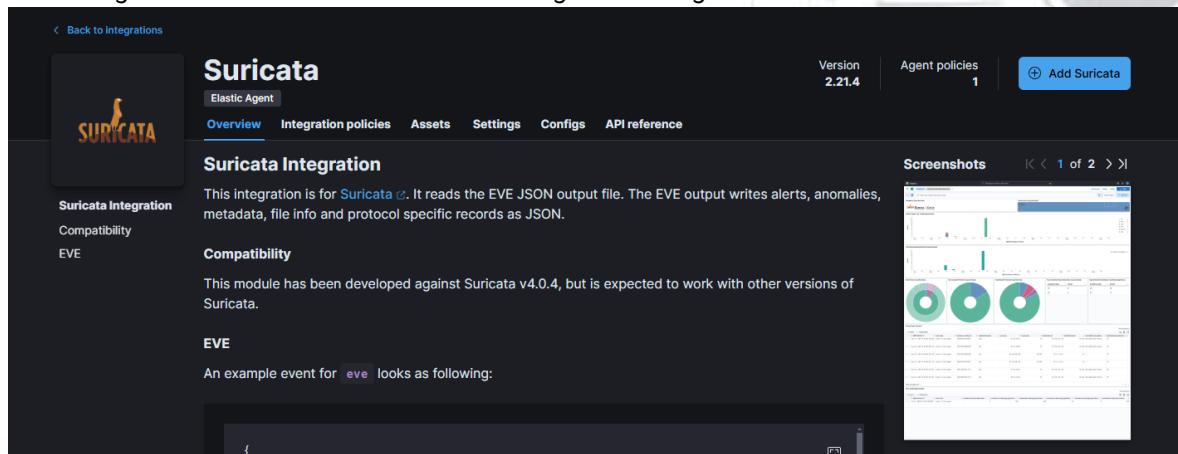
Una vez realizada la configuración encontraremos el siguiente panel.



The screenshot shows the Fleet interface for managing Elastic Agents. At the top, there are tabs for Agents, Agent policies, Enrollment tokens, Uninstall tokens, Data streams, and Settings. Below the tabs, there are two main sections: Ingest Overview Metrics and Agent Info Metrics. A search bar displays the policy ID: fleet-agents.policy_id : 502b3b85-ea1-4ea1-88ce-45a97f81522f. Below the search bar, it says 'Showing 1 agent'. There is a 'Clear filters' button and a status summary: 1 Healthy, 0 Unhealthy, 0 Updating, 0 Offline, 0 Inactive, 0 Unenrolled. A table lists the single agent: 'Status' (Healthy), 'Host' (kali), 'Agent policy' (Suricata/Linux rev. 2), 'CPU' (4.95 %), 'Memory' (230 MB), 'Last activity' (37 seconds ago), and 'Version' (8.17.0). There is also an 'Actions' column with a three-dot menu icon. At the bottom, there is a 'Rows per page: 20' dropdown and a navigation bar with arrows.

Integraciones Suricata

Para el Agent Suricata/Linux utilizaremos la siguiente integración.



The screenshot shows the Suricata integration page. At the top, there is a sidebar with 'Suricata Integration', 'Compatibility', and 'EVE'. The main content area has a title 'Suricata' with a 'Version 2.21.4' badge and an 'Agent policies 1' badge. There is a 'Add Suricata' button. Below the title, there are tabs for 'Overview', 'Integration policies', 'Assets', 'Settings', 'Configs', and 'API reference'. The 'Overview' tab is selected. It contains sections for 'Suricata Integration' (describing it as reading EVE JSON output file), 'Compatibility' (noting compatibility with Suricata v4.0.4), and 'EVE' (showing an example event structure). To the right, there is a 'Screenshots' section with a preview of the Suricata interface showing various dashboards and data visualizations.



Desde el apartado Discover podremos ver los Log de nuestro Suricata enlazado en Elastic

Documents (1,485)	Patterns	Field statistics
@timestamp	Jan 18, 2025 @ 22:46:10.856	#timestamp Jan 18, 2025 @ 22:46:10.856 agent:ephemeral_id 92982193-624b-4cdd-8175-dd9384838cf
		a agent.id b66781d2-df3c-43ab-9662-d595e3eebb1 agent.name kali agent.type filebea
		t agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default..
	✓ Jan 18, 2025 @ 22:46:09.946	#timestamp Jan 18, 2025 @ 22:46:09.946 agent:ephemeral_id 92982193-624b-4cdd-8175-dd9384838cf
		a agent.id b66781d2-df3c-43ab-9662-d595e3eebb1 agent.name kali agent.type filebea
		t agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default..
	✓ Jan 18, 2025 @ 22:46:09.841	#timestamp Jan 18, 2025 @ 22:46:09.841 agent:ephemeral_id 92982193-624b-4cdd-8175-dd9384838cf
		a agent.id b66781d2-df3c-43ab-9662-d595e3eebb1 agent.name kali agent.type filebea
		t agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default..
	✓ Jan 18, 2025 @ 22:46:09.840	#timestamp Jan 18, 2025 @ 22:46:09.840 agent:ephemeral_id 92982193-624b-4cdd-8175-dd9384838cf
		a agent.id b66781d2-df3c-43ab-9662-d595e3eebb1 agent.name kali agent.type filebea
		t agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default..

La integración ya dispone del path de logs, por lo que no tendremos que realizar modificaciones.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name
suricata-1

Description Optional

Collect Suricata eve logs (input: logfile) Change defaults ▾

Suricata eve logs (log) Collect Suricata eve logs using log input

Paths /var/log/suricata/eve.json

Preserve original event Preserves a raw copy of the original event, added to the field event.original

Where to add this integration?

Integraciones para Wind11

Para el Agent Wind11 utilizaremos la siguiente integración.

The screenshot shows the 'Windows' integration page under the 'Elastic Agent' section. The top navigation bar includes 'Back to Integrations', 'Windows' (selected), 'Overview' (highlighted in blue), 'Integration policies', 'Assets', 'Settings', 'Configs', and 'API reference'. The top right shows 'Version 2.3.6', 'Agent policies 1', and a blue button '+ Add Windows'. On the left, a sidebar titled 'Windows Integration' lists 'Data streams', 'Requirements', 'Setup', 'Ingesting Wind...', 'Notes', 'Windows Event ...', and 'Logs reference'. The main content area is titled 'Windows Integration' and describes how it allows monitoring Windows OS services, applications, and more. It includes a note about collecting metrics and logs from the machine, creating alerts, and troubleshooting issues. A screenshot of the Kibana Metrics Windows Services dashboard is shown on the right, displaying various service status metrics. Below the screenshot is a 'Details' link.

Aquí no será necesario modificar datos, ya que la configuración default es correcta.

The screenshot shows the 'Edit Windows integration' configuration page. The title is 'Edit Windows integration' with a 'Cancel' button. Below it is a sub-section 'Configure integration' with a step indicator '1'. The 'Integration settings' section asks to choose a name and description for identification. It shows 'Integration name: windows-2' and an 'Optional' 'Description' field. An 'Advanced options' link is visible. The 'Collect events from the following Windows event log channels:' section has a checked checkbox and a 'Change defaults' link. It lists 'AppLocker/EXE and DLL' and 'Microsoft-Windows-AppLocker/EXE and DLL' with their respective checkboxes. A 'Preserve original event' checkbox is also present with its description.

Integraciones para Honeypot

Para el Agent Honeypot utilizaremos la siguiente integración (custom)

The screenshot shows the 'Custom Logs' integration page. At the top, there's a lock icon and a navigation bar with 'Back to integrations'. Below the title 'Custom Logs' (with 'Elastic Agent' subtext), there are tabs for 'Overview', 'Integration policies', 'Assets', 'Settings', and 'Configs'. The 'Overview' tab is selected. On the left, there's a sidebar with 'Custom Logs Packa...', 'Get started', and 'ECS Field Mapping'. The main content area has a section titled 'Custom Logs Package' with instructions for using the package to ingest arbitrary log files. To the right, there's a 'Details' panel showing version 2.3.3, category 'Custom, Custom Logs', and other metadata like developer information and changelog links.

Asignaremos el siguiente path con las configuraciones adicionales
"/home/kali/cowrie_docker/logs/"

The screenshot shows the 'Edit Custom Logs integration' configuration screen. It starts with a 'Cancel' button and a title 'Edit Custom Logs integration'. Below that, it says 'Modify integration settings and deploy changes to the selected agent policy.' A step indicator '1 Configure integration' is shown. The 'Integration settings' section allows setting an 'Integration name' (log-1) and an optional 'Description'. An 'Advanced options' link is available. The 'Custom log file' section is active, indicated by a checked toggle switch. It includes a 'Change defaults' button, a 'Log file path' input field containing '/home/kali/cowrie_docker/logs/', a '+ Add row' button, and a note about the path being the 'Path to log files to be collected'. The 'Dataset name' is set to 'generic'. A note at the bottom states 'Set the name for your dataset. Changing the dataset will ...'.

Nuestra configuración queda evidenciada en el siguiente panel.

Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings

Ingest Overview Metrics Agent Info Metrics Agent activity Add Fleet

Filter your data using KQL syntax Status 4 Tags 0 Agent policy

Showing 4 agents Clear filters

Status	Host	Agent policy	CPU	Memory	Last activity	Version
Healthy	kali	Honeypot/Cowie rev. 2	2.20 %	213 MB	20 seconds ago	8.17.0
Healthy	DESKTOP-NA5TU51	Wind11 rev. 3	3.23 %	193 MB	35 seconds ago	8.17.0
Healthy	kali	Suricata/Linux rev. 2	1.60 %	202 MB	28 seconds ago	8.17.0
Healthy	10f63e3b3e9c	Elastic Cloud agent policy rev. 5	N/A	N/A	18 seconds ago	8.17.0

Rows per page: 20

LOGS – Elastic.

Revisaremos los logs desde el apartado Discover > Search.

Suricata:



Copiaremos los valores desde Elastic y los incluimos en fichero "LogElastic_Suricata.txt"

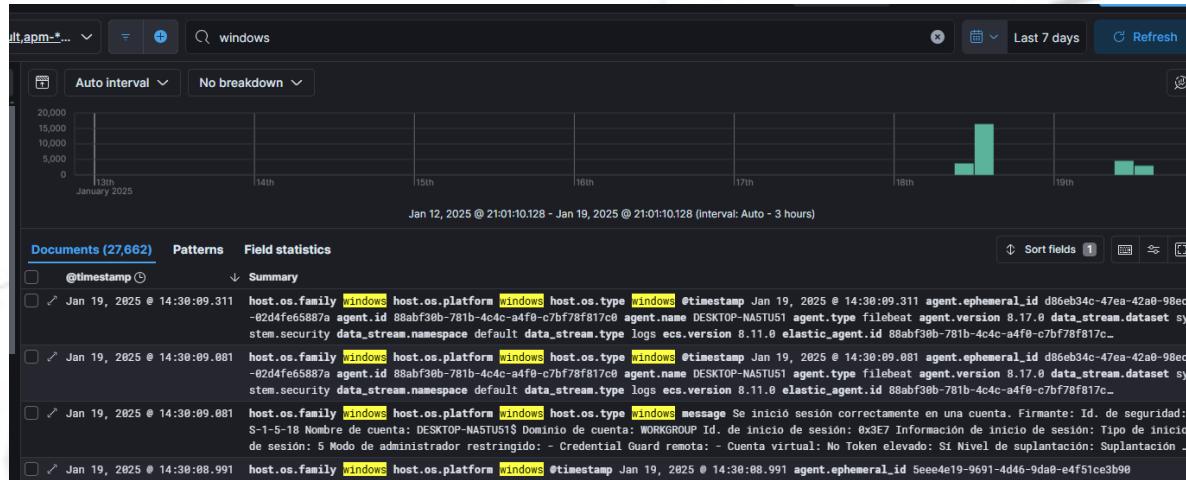
The screenshot shows the Elasticsearch UI with a selected log document. The document's _source field is displayed in a code editor-like interface. The "elastic_agent.version" field is highlighted in yellow. A "Copy value" button is visible at the bottom left of the code editor.

```
{
  "_index": "ds-logs-elastic_agent-default-2025.01.18-000001",
  "_id": "ijjlfpQBV3JqTxqr4U04",
  "_version": 1,
  "_score": null,
  "fields": {
    "elastic_agent.version": [
      "8.17.0"
    ]
  }
}
```

Copy value

```
8.17.0 agent.ephemeral_id bc9e4b83-114c-4061-8a55-695t agent.version 8.17.0 component.id log-default component.state
```

Wind11:



Copiaremos los valores desde Elastic y los incluiremos en fiche "LogElastic_Wind11.txt"

The screenshot shows the Elasticsearch interface with a search results table. One row is selected, showing a detailed view of the log entry. The selected log entry is:

```
{  
  "_index": ".ds-logs-system.  
  security-default-2025.01.19-000001",  
  "_id": "SS7ffpQBYMqPPj5oaGmj",  
  "_version": 1,  
  "_score": null,  
  "fields": {  
    "elastic_agent.version": [  
      "8.17.0"  
    ]  
  }  
}
```

Below the table is a button labeled "Copy value".

Considerando problemas en migrar los logs desde Kali a Elastic, comparto el archivo manual de los logs realizado en la máquina.

```
(kali㉿kali)-[~] $ docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
e4afb7e25116 cowrie/cowrie:latest "/cowrie/cowrie-env/..." 2 minutes ago Up 2 minutes 2222/tcp cool_dewdney
(kali㉿kali)-[~] $ docker logs e4afb7e25116
```

```
(kali㉿kali)-[~] out reached in HoneyPotSSHTransport
$ docker logs e4afb7e25116 > ~/Desktop/cowrie_logs.txt
./cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:105: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
    b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
./cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:112: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
    b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
```

Adjunto el Archivo con el resto de la información.

RESUMEN.

Diagramamos una infraestructura para conectando 3 redes al UTM pfSense, entendiendo las limitaciones de una red doméstica.

Creamos el UTM desde la ISO (pfSense) simulando un entorno laboral, con la posibilidad de dirigir, redirigir, cancelar, bloquear y controlar las conexiones internas y externas.

Definimos las configuraciones para cada máquina según el requerimiento solicitado (conexiones y restricciones).

Asignamos reglas de Firewall para cada acceso y definimos una IP estática para conectarse desde una red externa.

Activamos y configuramos Elastic, definiendo integraciones para cada máquina virtual.

Enrollamos cada maquina con el server de Elastic para enviar, almacenar y analizar los logs de cada una.

Herramientas Utilizadas

- Virtual Box
- MV_UTM-01
- MV_Kali
- MV_Wind11
- <https://www.elastic.co/es/cloud>
- GitHub

Ficheros Entregados

- Practica Blue Team.docx
- LogElastic_suricata.txt
- LogElastic_Wind11.txt
- LogCowrie.txt